SonicWALL Network Security Appliances

NETWORK SECURITY

NSA 2400

Getting Started Guide

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL NSA 2400 Getting Started Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWALL Network Security Appliance (NSA) 2400 running SonicOS Enhanced. After you complete this guide, computers on your Local Area Network (LAN) will have secure Internet access.

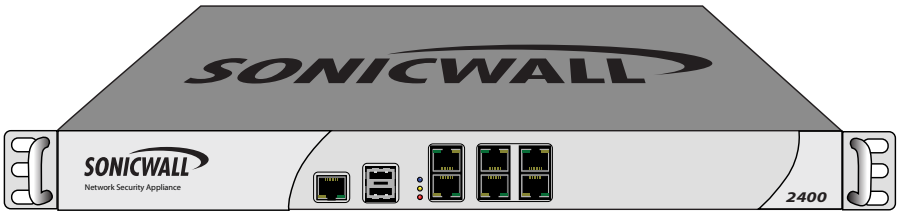
Document Contents

This document contains the following sections:

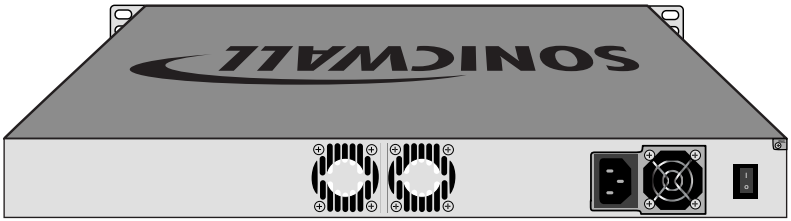
1. *Pre-Configuration Tasks* - page 3
2. *Registering Your Appliance on MySonicWALL* - page 9
3. *Deployment Scenarios* - page 14
4. *Additional Deployment Configuration* - page 35
5. *Support and Training Options* - page 55
6. *Product Safety and Regulatory Information* - page 63

SonicWALL NSA 2400 Overview

Front



Back



Form Factor	1U rack-mountable
Dimensions	17 x 10.25 x 1.75 in 43.18 x 26.04 x 4.44 cm
Weight	8.05 lbs/ 3.71 kg
WEEE Weight	8.05 lbs/ 3.71 kg
Voltage	1 Amp / 50-60Hz

Note: *Always observe proper safety and regulatory guidelines when removing administrator-serviceable parts from the SonicWALL NSA appliance. Proper guidelines can be found in the Safety and Regulatory Information section, on page 64 of this guide.*

Pre-Configuration Tasks 1

In this Section:

This section provides pre-configuration information. Review this section before setting up your SonicWALL NSA 2400 appliance.

- *Check Package Contents* - page 4
- *Obtain Configuration Information* - page 5
- *The Front Panel* - page 6
- *The Back Panel* - page 7

Check Package Contents

Before setting up your SonicWALL NSA appliance, verify that your package contains the following parts:

1. NSA 2400 Appliance
2. DB9 -> RJ45 (CLI) Cable
3. Power Cord*
4. Standard Ethernet Cable
5. Red Crossover Cable
6. Getting Started Guide
7. Rack Mount Kit **

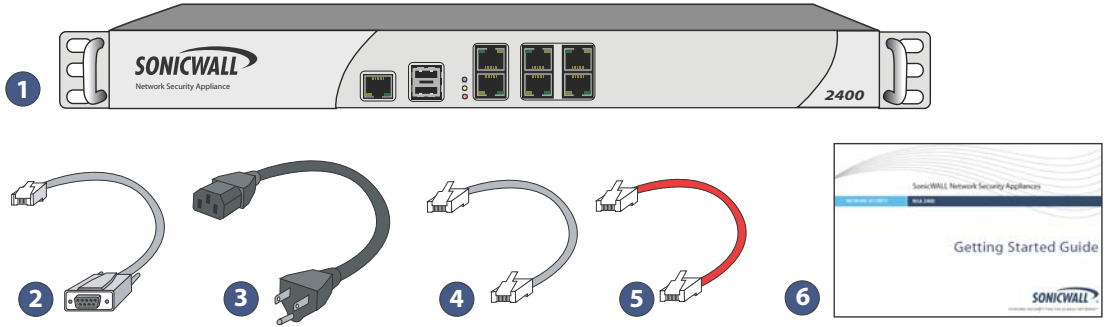
Any Items Missing?

If any items are missing from your package, please **contact SonicWALL support**.

A listing of the most current support documents are available online at: <http://www.sonicwall.com/us/support.html>

*The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
*Das beigefügte Netzkabel ist nur für den Gebrauch in Nordamerikas Vorgesehen. Für Kunden in der Europaïschen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.

**This item is not included in the below illustration.



Obtain Configuration Information

Please record and keep for future reference the following setup information:

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your SonicWALL appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your SonicWALL appliance.

Networking Information

LAN IP Address: _____._____._____._____	Select a static IP address for your SonicWALL appliance that is within the range of your local subnet. If you are unsure, you can use the default IP address (192.168.168.168).
Subnet Mask: _____._____._____._____	Record the subnet mask for the local subnet where you are installing your SonicWALL appliance.
Ethernet WAN IP Address: _____._____._____._____	Select a static IP address for your Ethernet WAN. *This setting only applies if you are already using an ISP that assigns a static IP address.*

Administrator Information

Admin Name:	Select an administrator account name. (default is *admin)*
Admin Password:	Select an administrator password. (default is *password*)

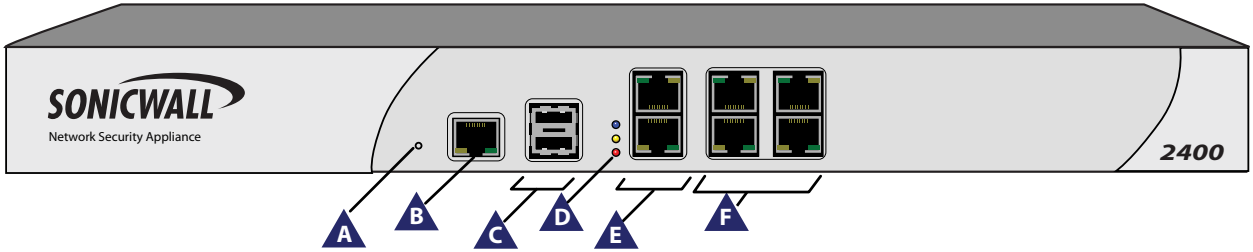
Obtain Internet Service Provider (ISP) Information

Record the following information about your current Internet service:

If you connect using	Please record
DHCP	*No information is usually required*: Some providers may require a Host name: _____
Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway: _____._____._____._____ Primary DNS: _____._____._____._____ DNS 2 (optional): _____._____._____._____ DNS 3 (optional): _____._____._____._____

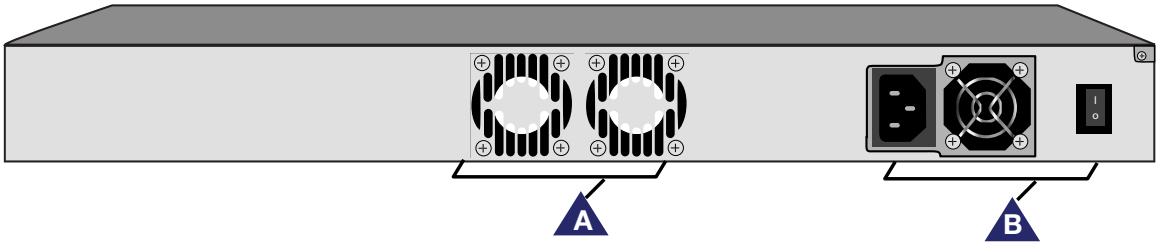
Note: *If you are not using one of the network configurations above, refer to* <http://www.sonicwall.com/us/support.html>.

The Front Panel



Icon	Feature	Description
A	**Reset Button**	Press and hold the button for a few seconds to manually reset the appliance using SafeMode.
B	**Console Port**	Used to access the SonicOS Command Line Interface (CLI) via the DB9 -> RJ45 cable.
C	**USB Ports (2)**	For future use.
D	**LED** (Top to Bottom)	**Power LED:** Indicates the SonicWALL NSA appliance is powered on. **Test LED: Flickering**: Indicates the appliance is initializing. **Steady blinking**: Indicates the appliance is in SafeMode. **Solid**: Indicates that the appliance is in test mode. **Alarm LED:** Indicates an alarm condition.
E	**X0 (LAN), X1 (WAN)**	Gigabit Ethernet ports for LAN and WAN connections.
F	**X2-X5 (LAN)**	Gigabit Ethernet ports for other configurable Ethernet connections.

The Back Panel



Icon	Feature	Description
A	**Fans(2)**	The SonicWALL NSA 2400 includes two fans for system temperature control.
B	**Power Supply**	The SonicWALL NSA 2400 power supply.

Before You Register

You need a MySonicWALL account to register the SonicWALL NSA appliance. You can create a new MySonicWALL account on www.mysonicwall.com or directly from the SonicWALL management interface. This section describes how to create an account by using the Web site.

If you already have a MySonicWALL account, go to *Registering and Licensing Your Appliance on MySonicWALL* - page 10 to register your appliance on MySonicWALL. You can also postpone registration until after having set up the appliance. Skip ahead to *Deployment Scenarios* - page 14 and register your appliance directly from the management interface once you reach *Accessing the Management Interface* - page 20.

Note: *For a High Availability configuration, you must use MySonicWALL to associate a backup unit that can share the Security Services licenses with your primary SonicWALL.*

If you do not yet have a MySonicWALL account, you can use MySonicWALL to register your SonicWALL appliance and activate or purchase licenses for Security Services, ViewPoint Reporting and other services, support, or software before you even connect your device. This method allows you to prepare for your deployment before making any changes to your existing network.

Note: *Your SonicWALL NSA appliance does not need to be powered on during account creation or during the MySonicWALL registration and licensing process.*

After registering a new SonicWALL appliance on MySonicWALL, you must also register the appliance from the SonicOS management interface. This allows the unit to synchronize with the SonicWALL License Server and to share licenses with the associated appliance, if any. See *Accessing the Management Interface* - page 20.

Registering Your Appliance on MySonicWALL

2

In this Section:

This section provides instructions for registering your SonicWALL NSA 2400 appliance.

- *Before You Register* - page 8
- *Creating a MySonicWALL Account* - page 10
- *Registering and Licensing Your Appliance on MySonicWALL* - page 10
- *Licensing Security Services and Software* - page 11
- *Registering a Second Appliance as a Backup* - page 12
- *Registration Next Steps* - page 13

Note: *Registration is an important part of the setup process and is necessary in order to receive the benefits of SonicWALL security services, firmware updates, and technical support.*

Creating a MySonicWALL Account

To create a MySonicWALL account, perform the following steps:

1. In your browser, navigate to www.mysonicwall.com.
2. In the login screen, click **If you are not a registered user, Click here**.

3. Complete the Registration form and then click **Register**.
4. Verify that the information is correct and then click **Submit**.
5. In the screen confirming that your account was created, click **Continue**.

Registering and Licensing Your Appliance on MySonicWALL

This section contains the following subsections:

- *Product Registration* - page 10
- *Licensing Security Services and Software* - page 11
- *Managing Licenses* - page 11
- *Registering a Second Appliance as a Backup* - page 12

Product Registration

You must register your SonicWALL security appliance on MySonicWALL to enable full functionality.

1. Login to your MySonicWALL account. If you do not have an account, you can create one at www.mysonicwall.com.
2. On the main page, in the **Register A Product** field, type the appliance serial number and then click **Next**.
3. On the My Products page, under **Add New Product**, type the friendly name for the appliance, select the **Product Group** if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**.

Licensing Security Services and Software

The Service Management - Associated Products page in MySonicWALL lists security services, support options, and software such as ViewPoint that you can purchase or try with a free trial. For details, click the **Info** button. Your current licenses are indicated in the **Status** column with either a license key or an expiration date. You can purchase additional services now or at a later time.

The following products and services are available for the SonicWALL NSA 2400:

- **Service Bundles:**
  - Client/Server Anti-Virus Suite
  - Comprehensive Gateway Security Suite
- **Gateway Services:**
  - Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Firewall
  - Global Management System
  - Content Filtering: Premium Edition
  - Stateful High Availability Upgrade
- **Desktop and Server Software:**
  - Enforced Client Anti-Virus and Anti-Spyware
  - Global VPN Client
  - Global VPN Client Enterprise
  - ViewPoint
- **Support Services:**
  - Dynamic Support 8x5
  - Dynamic Support 24x7
  - Software and Firmware Updates

Managing Licenses

To manage your licenses, perform the following tasks:

1. In the MySonicWALL Service Management - Associated Products page, check the **Applicable Services** table for services that your SonicWALL appliance is already licensed for. Your initial purchase may have included security services or other software bundled with the appliance. These licenses are enabled on MySonicWALL when the SonicWALL appliance is delivered to you.
2. If you purchased a service subscription or upgrade from a sales representative separately, you will have an **Activation Key** for the product. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase. Locate the product on the Service Management page and click **Enter Key** in that row.
3. In the Activate Service page, type or paste your key into the **Activation Key** field and then click **Submit**. Depending on the product, you will see an expiration date or a license key string in the **Status** column when you return to the Service Management page.

4. To license a product of service, do one of the following:
   - To try a Free Trial of a service, click **Try** in the Service Management page. A 30-day free trial is immediately activated. The Status page displays relevant information including the activation status, expiration date, number of licenses, and links to installation instructions or other documentation. The Service Management page is also updated to show the status of the free trial.
   - To purchase a product or service, click **Buy Now**.
5. In the Buy Service page, type the number of licenses you want in the **Quantity** column for either the 1 year, 2 year, or 3 year license row and then click **Add to Cart.**
6. In the Checkout page, follow the instructions to complete your purchase.

The MySonicWALL server will generate a license key for the product. The key is added to the license keyset. You can use the license keyset to manually apply all active licenses to your SonicWALL appliance.

For more information, see *Registration Next Steps* - page 13.

Registering a Second Appliance as a Backup

To ensure that your network stays protected if your SonicWALL appliance has an unexpected failure, you can purchase a license to associate a second SonicWALL of the same model as the first in a high availability (HA) pair. You can purchase the license associate the two appliances as part of the registration process on MySonicWALL. The second SonicWALL will automatically share the Security Services licenses of the primary appliance.

To register a second appliance and associate it with the primary, perform the following steps:

1. Login to your MySonicWALL account.
2. On the main page, in the Register A Product field, type the appliance serial number and then click **Next**.
3. On the My Products page, under Add New Product, type the friendly name for the appliance, select the Product Group if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**. The Create Association Page is displayed.
5. On the Create Association Page, click the radio button to select the primary unit for this association, and then click **Continue**. The screen only displays units that are not already associated with other appliances.
6. On the Service Management - Associated Products page, scroll down to the Associated Products section to verify that your product registered successfully. You should see the HA Primary unit listed in the Parent Product section, as well as a Status value of **0** in the Associated Products / Child Product Type section.
7. Although the Stateful High Availability Upgrade and all the Security Services licenses can be shared with the HA Primary unit, you must purchase a separate ViewPoint

license for the backup unit. This will ensure that you do not miss any reporting data in the event of a failover. Under Desktop & Server Software, click **Buy Now** for ViewPoint. Follow the instructions to complete the purchase.

To return to the Service Management - Associated Products page, click the serial number link for this appliance.

Registration Next Steps

Your SonicWALL NSA 2400 HA Pair is now registered and licensed on MySonicWALL. To complete the registration process in SonicOS and for more information, see:

- *Accessing the Management Interface* - page 20
- *Activating Licenses in SonicOS* - page 22
- *Enabling Security Services in SonicOS* - page 41
- *Enforcing Security Services on Network Zones* - page 45

Deployment Scenarios 3

In this Section:

This section provides detailed overviews of advanced deployment scenarios and configuration instructions for connecting your SonicWALL NSA 2400.

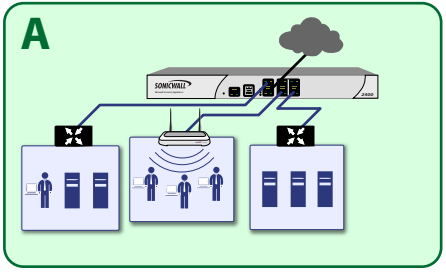
- *Selecting a Deployment Scenario* - page 15
  - *Scenario A: NAT/Route Mode Gateway* - page 16
  - *Scenario B: State Sync Pair in NAT/Route Mode* - page 17
  - *Scenario C: L2 Bridge Mode* - page 18
- *Initial Setup* - page 19
- *Upgrading Firmware on Your SonicWALL* - page 26
- *Configuring a State Sync Pair in NAT/Route Mode* - page 31
- *Configuring L2 Bridge Mode* - page 31

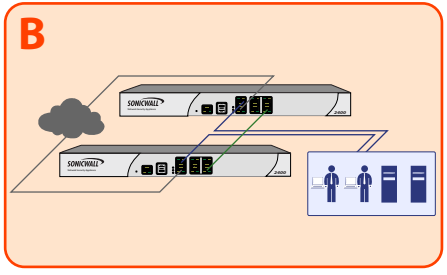
Tip: *Before completing this section, fill out the information in Obtain Configuration Information - page 5. You will need to enter this information during the **Setup Wizard**.*

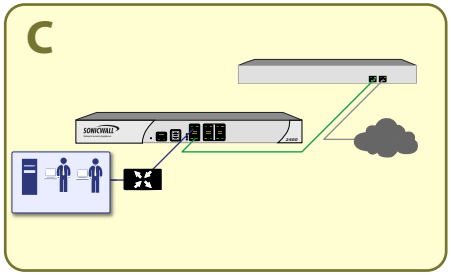
Selecting a Deployment Scenario

Before continuing, select a deployment scenario that best fits your network scheme. Reference the table below and the diagrams on the following pages for help in choosing a scenario.

Current Gateway Configuration	New Gateway Configuration	Use Scenario
No gateway appliance	Single SonicWALL NSA as a primary gateway.	**A** - NAT/Route Mode Gateway
	Pair of SonicWALL NSA appliances for high availability.	**B** - NAT with State Sync Pair
Existing Internet gateway appliance	SonicWALL NSA as replacement for an existing gateway appliance.	**A** - NAT/Route Mode Gateway
	SonicWALL NSA in addition to an existing gateway appliance.	**C** - Layer 2 Bridge Mode
Existing SonicWALL gateway appliance	SonicWALL NSA in addition to an existing SonicWALL gateway appliance.	**B** - NAT with State Sync Pair





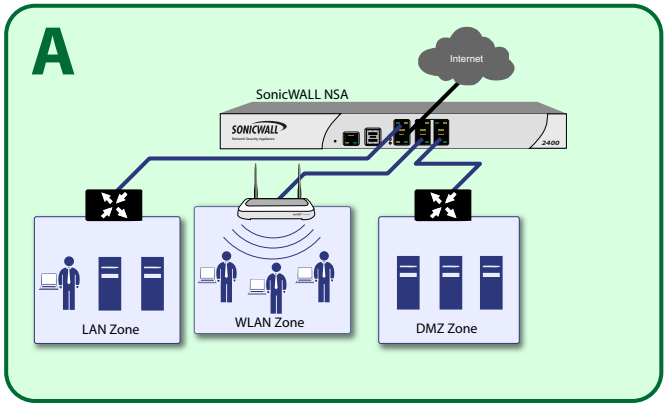


Scenario A: NAT/Route Mode Gateway

For new network installations or installations where the SonicWALL NSA 2400 is replacing the existing network gateway.

In this scenario, the SonicWALL NSA 2400 is configured in NAT/Route mode to operate as a single network gateway. Two Internet sources may be routed through the SonicWALL appliance for load balancing and failover purposes. Because only a single SonicWALL appliance is deployed, the added benefits of high availability with a stateful synchronized pair are not available.

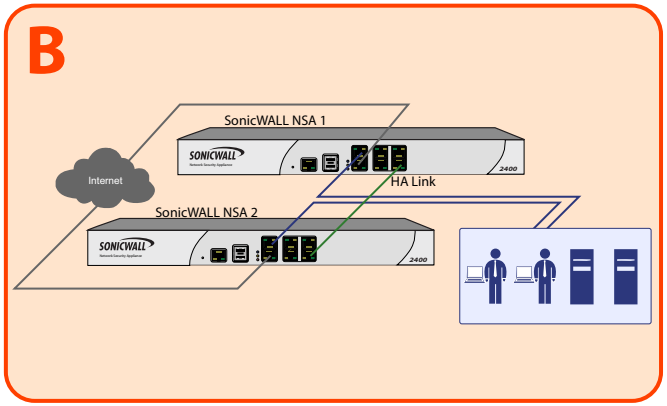
To set up this scenario, follow the steps covered in *Initial Setup* - page 19. If you have completed setup procedures in that section, continue to *Additional Deployment Configuration* - page 35 to complete configuration.



Scenario B: State Sync Pair in NAT/Route Mode

For network installations with two SonicWALL NSA 2400 appliances configured as a stateful synchronized pair for redundant high-availability networking.

In this scenario, one SonicWALL NSA 2400 operates as the primary gateway device and the other SonicWALL NSA 2400 is in passive mode. All network connection information is synchronized between the two devices so that the backup appliance can seamlessly switch to active mode without dropping any connections if the primary device loses connectivity.



To set up this scenario, follow the steps covered in the *Initial Setup* - page 19 and the *Configuring a State Sync Pair in NAT/Route Mode* - page 26 sections. If you have completed setup procedures in those sections, continue to the *Additional Deployment Configuration* - page 35 to complete configuration.

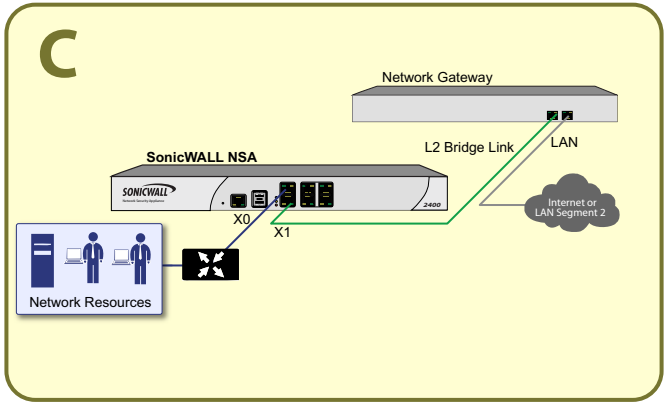
Scenario C: L2 Bridge Mode

For network installations where the SonicWALL NSA 2400 is running in tandem with an existing network gateway.

In this scenario, the original gateway is maintained. The SonicWALL NSA 2400 is integrated seamlessly into the existing network, providing the benefits of deep packet inspection and comprehensive security services on all network traffic.

L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWALL security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast and IPv6.

To set up this scenario, follow the steps covered in the *Initial Setup* - page 19 and the *Configuring L2 Bridge Mode* - page 31 sections. If you have completed setup procedures in those sections, continue to the *Additional Deployment Configuration* - page 35 to complete configuration.



Initial Setup

This section provides initial configuration instructions for connecting your SonicWALL NSA 2400. Follow these steps if you are setting up **scenario A**, **B**, or **C**.

This section contains the following subsections:

- *System Requirements* - page 19
- *Connecting the WAN Port* - page 19
- *Connecting the LAN Port* - page 20
- *Applying Power* - page 20
- *Accessing the Management Interface* - page 20
- *Using the Setup Wizard* - page 21
- *Connecting to Your Network* - page 22
- *Testing Your Connection* - page 22
- *Activating Licenses in SonicOS* - page 22
- *Upgrading Firmware on Your SonicWALL* - page 23

System Requirements

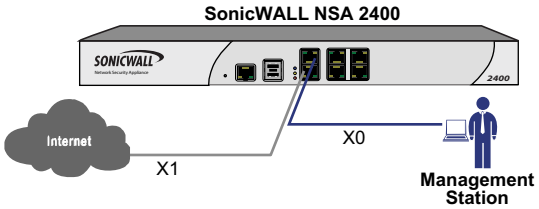
Before you begin the setup process, check to verify that you have:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads

	Accepted Browser	Browser Version Number
	Internet Explorer	6.0 or higher
	Firefox	2.0 or higher
	Netscape	9.0 or higher
	Opera	9.10 or higher for Windows
	Safari	2.0 or higher for MacOS

Connecting the WAN Port

1. Connect one end of an Ethernet cable to your Internet connection.
2. Connect the other end of the cable to the **X1** (**WAN**) port on your SonicWALL NSA Series appliance.



Connecting the LAN Port

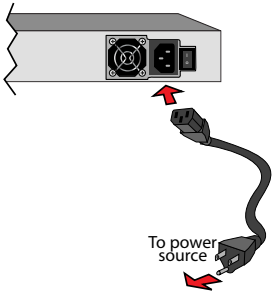
1. Connect one end of the provided Ethernet cable to the computer you are using to manage the SonicWALL NSA Series.
2. Connect the other end of the cable to the **X0** port on your SonicWALL NSA Series.

   The Link LED above the **X0** (**LAN**) port will light up in green or amber depending on the link throughput speed, indicating an active connection:

   - Amber indicates 1 Gbps
   - Green indicates 100 Mbps
   - Unlit while the right (activity) LED is illuminated indicates 10 Mbps

Applying Power

1. Plug the power cord into an appropriate power outlet.
2. Turn on the power switch on the rear of the appliance next to the power cords.



The Power LED on the front panel lights up blue when you plug in the SonicWALL NSA. The Alarm LED may light up and the Test LED will light up and may blink while the appliance performs a series of diagnostic tests.

When the Power LEDs are lit and the Test LED is no longer lit, the SonicWALL NSA is ready for configuration. This typically occurs within a few minutes of applying power to the appliance.

Note: *If the Test or Alarm LEDs remain lit after the SonicWALL NSA appliance has been booted, restart the appliance by cycling power.*

Accessing the Management Interface

The computer you use to manage the SonicWALL NSA Series must be set up to have an unused IP address on the 192.168.168.x/24 subnet, such as 192.168.168.20.

To access the SonicOS Enhanced Web-based management interface:

1. Start your Web browser.

Note: *Disable pop-up blocking software or add the management IP address http://192.168.168.168 to your pop-up blocker's allow list.*

2. Enter **http://192.168.168.168** (the default LAN management IP address) in the **Location** or **Address** field.
3. The **SonicWALL Setup Wizard** launches and guides you through the configuration and setup of your SonicWALL NSA appliance.

   The **Setup Wizard** launches only upon initial loading of the SonicWALL NSA management interface.
4. Follow the on-screen prompts to complete the Setup Wizard.

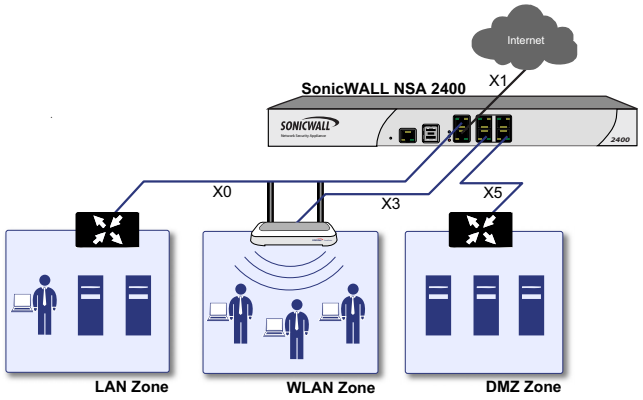
Depending on the changes made during your setup configuration, the SonicWALL may restart.

Using the Setup Wizard

If you cannot connect to the SonicWALL NSA appliance or the **Setup Wizard** does not display, verify the following configurations:

- Did you correctly enter the management IP address in your Web browser?
- Are the Local Area Connection settings on your computer set to use DHCP or set to a static IP address on the 192.168.168.x/24 subnet?
- Do you have the Ethernet cable connected to your computer and to the **X0** (**LAN**) port on your SonicWALL?
- Is the connector clip on your network cable properly seated in the port of the security appliance?
- Some browsers may not launch the **Setup Wizard** automatically. In this case:
  - Log into SonicWALL NSA appliance using "**admin**" as the user name and "**password**" as the password.
  - Click the **Wizards** button on the **System** > **Status** page.
  - Select **Setup Wizard** and click **Next** to launch the Setup Wizard.
  - Some pop-up blockers may prevent the launch of the Setup Wizard. You can temporarily disable your pop-up blocker, or add the management IP address of your SonicWALL (192.168.168.168 by default) to your pop-up blocker's allow list.

Connecting to Your Network



The SonicWALL NSA 2400 ships with the internal DHCP server active on the LAN port. However, if a DHCP server is already active on your LAN, the SonicWALL will disable its own DHCP server to prevent conflicts.

Ports X1 and X0 are preconfigured as WAN and LAN. The remaining ports (X2-X5) can be configured to meet the needs of your network. As an example, zones in the example above are configured as:

- X1: WAN
- X2: LAN
- X3: WLAN
- X5: DMZ

Testing Your Connection

1. After you exit the Setup Wizard, the login page reappears. Log back into the Management Interface and verify your IP and WAN connection.
2. Ping a host on the Internet, such as sonicwall.com.
3. Open another Web browser and navigate to: <http://www.sonicwall.com>.

   If you can view the SonicWALL home page, you have configured your SonicWALL NSA appliance correctly.

   If you cannot view the SonicWALL home page, renew your management station DHCP address.
4. If you still cannot view a Web page, try one of these solutions:
   - **Restart your Management Station** to accept new network settings from the DHCP server in the SonicWALL security appliance.
   - **Restart your Internet Router** to communicate with the DHCP Client in the SonicWALL security appliance.

Activating Licenses in SonicOS

After completing the registration process in SonicOS, you must perform the following tasks to activate your licenses and enable your licensed services from within the SonicOS user interface:

- Activate licenses
- Enable security services
- Apply services to network zones

This section describes how to activate your licenses. For instructions on how to enable security services and apply services to network zones, see the following sections:

- *Enabling Security Services in SonicOS* - page 41
- *Enforcing Security Services on Network Zones* - page 45

To activate licensed services in SonicOS, you can enter the license keyset manually, or you can synchronize all licenses at once with MySonicWALL.

The Setup Wizard automatically synchronizes all licenses with MySonicWALL if the appliance has Internet access during initial setup. If initial setup is already complete, you can synchronize licenses from the **System** > **Licenses** page.

Manual upgrade using the license keyset is useful when your appliance is not connected to the Internet. The license keyset includes all license keys for services or software enabled on MySonicWALL. It is available on <http://www.sonicwall.com> at the top of the Service Management page for your SonicWALL NSA appliance.

To activate licenses in SonicOS:

1. Navigate to the **System** > **Licenses** page.
2. Under Manage Security Services Online do one of the following:
   - Enter your MySonicWALL credentials, then click the **Synchronize** button to synchronize licenses with MySonicWALL.
   - Paste the license keyset into the **Manual Upgrade Keyset** field.
3. Click **Submit**.

Upgrading Firmware on Your SonicWALL

The following procedures are for upgrading an existing SonicOS Enhanced image to a newer version:

- *Obtaining the Latest Firmware* - page 23
- *Saving a Backup Copy of Your Preferences* - page 24
- *Upgrading the Firmware with Current Settings* - page 24
- *Upgrading the Firmware with Factory Defaults* - page 25
- *Using SafeMode to Upgrade Firmware* - page 25

Obtaining the Latest Firmware

1. To obtain a new SonicOS Enhanced firmware image file for your SonicWALL security appliance, connect to your MySonicWALL account at <http://www.mysonicwall.com>.
2. Copy the new SonicOS Enhanced image file to a convenient location on your management station.

Saving a Backup Copy of Your Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of the current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state. The System Backup shows you the current configuration and firmware in a single, clickable restore image.

In addition to using the backup feature to save your current configuration state to the SonicWALL security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the SonicWALL security appliance.

Perform the following procedures to save a backup of your configuration settings and export them to a file on your local management station:

1. On the **System** > **Settings** page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the **Firmware Management** table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.

Upgrading the Firmware with Current Settings

Perform the following steps to upload new firmware to your SonicWALL appliance and use your current configuration settings upon startup.

Tip: *The appliance must be properly registered before it can be upgraded. Refer to Registering and Licensing Your Appliance on MySonicWALL - page 10 for more information.*

1. Download the SonicOS Enhanced firmware image file from MySonicWALL and save it to a location on your local computer.
2. On the **System** > **Settings** page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file and click the **Upload** button.
4. On the **System** > **Settings** page, click the **Boot** icon in the row for **Uploaded Firmware**.
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS Enhanced image version information is listed on the **System** > **Settings** page.

Upgrading the Firmware with Factory Defaults

Perform the following steps to upload new firmware to your SonicWALL appliance and start it up using the default configuration:

1. Download the SonicOS Enhanced firmware image file from MySonicWALL and save it to a location on your local computer.
2. On the **System** > **Settings** page, click **Create Backup**.
3. Click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file and click the **Upload** button.
5. On the **System** > **Settings** page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.
6. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
7. Enter the default user name and password (admin/password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware

If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System** > **Settings** page.

To use SafeMode to upgrade firmware on the SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 port on the SonicWALL appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. To configure the appliance in SafeMode, perform one of the following:
   - Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the front of the security appliance for one second. The reset button is in a small hole next to the USB ports.
   - The Test light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.
3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS Enhanced firmware image, select the file and click the **Upload** button.
6. Select the boot icon in the row for one of the following:
   - **Uploaded Firmware - New!**

     Use this option to restart the appliance with your current configuration settings.
   - **Uploaded Firmware with Factory Defaults - New!**

Use this option to restart the appliance with default configuration settings.

7. In the confirmation dialog box, click **OK** to proceed.
8. After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicWALL management interface.

If You Are Following Scenario...	Proceed to Section:
A - NAT/Route Mode Gateway	*Additional Deployment Configuration* - page 35
B - NAT with State Sync Pair	*Configuring a State Sync Pair in NAT/Route Mode* - page 26
C - L2 Bridge Mode	*Configuring L2 Bridge Mode* - page 31

Configuring a State Sync Pair in NAT/Route Mode

This section provides instructions for configuring a pair of SonicWALL NSA appliances for high availability (HA). This section is relevant to administrators following deployment **scenario B**.

This section contains the following subsections:

- *Initial High Availability Setup* - page 26
- *Configuring High Availability* - page 27
- *Configuring Advanced HA Settings* - page 27
- *Synchronizing Settings* - page 29
- *Synchronizing Firmware* - page 30
- *Configuring HA License Overview* - page 30
- *Associating Pre-Registered Appliances* - page 31

Initial High Availability Setup

Before you begin the configuration of HA on the Primary SonicWALL security appliance, perform the following setup:

1. On the back panel of the Backup SonicWALL security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability** > **Settings** page.
2. Verify that the Primary SonicWALL and Backup SonicWALL security appliances are registered, running the same SonicOS Enhanced versions, and running the same SonicWALL Security services.

3. Make sure the Primary SonicWALL and Backup SonicWALL security appliances' LAN, WAN and other interfaces are properly configured for failover.
4. Connect the X5 ports on the Primary SonicWALL and Backup SonicWALL appliances with a CAT6-rated crossover cable (red crossover cable). The Primary and Backup SonicWALL security appliances must have a dedicated connection. SonicWALL recommends cross-connecting the two together using a CAT 6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also valid.
5. Power up the Primary SonicWALL security appliance, and then power up the Backup SonicWALL security appliance.
6. Do not make any configuration changes to the Primary's X5; the High Availability configuration in an upcoming step takes care of this issue. When done, disconnect the workstation.

Configuring High Availability

The first task in setting up HA after initial setup is configuring the **High Availability** > **Settings** page on the Primary SonicWALL security appliance. Once you configure HA on the Primary SonicWALL security appliance, it communicates the settings to the Backup SonicWALL security appliance.

To configure HA on the Primary SonicWALL, perform the following steps:

1. Navigate to the **High Availability** > **Settings** page.
2. Select the **Enable High Availability** checkbox.
3. Under **SonicWALL Address Settings**, type in the serial number for the Backup SonicWALL appliance.

You can find the serial number on the back of the SonicWALL security appliance, or in the **System** > **Status** screen of the backup unit. The serial number for the Primary SonicWALL is automatically populated.

4. Click **Apply** to retain these settings.

Configuring Advanced HA Settings

1. Navigate to the **High Availability** > **Advanced** page.
2. To configure Stateful HA, select **Enable Stateful Synchronization**. A dialog box is displayed with recommended settings for the **Heartbeat Interval** and **Probe Interval** fields. The settings it shows are minimum recommended values. Lower values may cause unnecessary failovers, especially when the SonicWALL is under a heavy load. You can use higher values if your SonicWALL handles a lot of network traffic. Click **OK**.

Tip: *Preempt mode is automatically disabled after enabling Stateful Synchronization. This is because preempt mode can be over-aggressive about failing over to the backup appliance. For example if both devices are idle, preempt mode may prompt a failover.*

3. To backup the firmware and settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.
4. Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the WAN switch to which the two appliances are connected to needs to be notified. All outside devices will continue to route to the single shared MAC address.
5. The **Heartbeat Interval** controls how often the two units communicate. The default is 5000 milliseconds; the minimum recommended value is 1000 milliseconds. Less than this may cause unnecessary failovers, especially when the SonicWALL is under a heavy load.
6. Typically, SonicWALL recommends leaving the **Heartbeat Interval**, **Election Delay Time (seconds)**, and **Dynamic Route Hold-Down Time** fields to their default settings. These fields can be tuned later as necessary for your specific network environment:
   - The **Failover Trigger Level** sets the number of heartbeats that can be missed before failing over. By default, this is set to 5 missed heartbeats.
   - The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role.
   - The **Probe Level** sets the interval in seconds between communication with upstream or downstream systems. The default is 20 seconds, and the allowed range is 5 to 255 seconds. You can set the Probe IP Address(es) on the **High Availability** > **Monitoring** screen.
   - The **Dynamic Route Hold-Down Time** setting is used when a failover occurs on a HA pair that is using either RIP or OSPF dynamic routing, and it is only displayed when the **Advanced Routing** option is selected on the **Network** > **Routing** page. When a failover occurs, **Dynamic Route Hold-Down Time** is the number of seconds the newly-active appliance keeps the dynamic routes it had previously learned in its route table.
   - During this time, the newly-active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, it deletes the old routes and implements the new routes it has learned from RIP or OSPF. The default value is 45 seconds. In large or complex networks, a larger value may improve network stability during a failover.
7. Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
8. Click **Synchronize Settings** to synchronize the settings between the Primary and Backup appliances.
9. Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Secondary unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Secondary appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
10. Click **Apply** to retain the settings on this screen.

Synchronizing Settings

Once you have configured the HA setting on the Primary SonicWALL security appliance, click the **Synchronize Settings** button. You should see a **HA Peer Firewall has been updated** message at the bottom of the management interface page. Also note that the management interface displays **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that certificates, certificate revocation lists (CRL) and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the Primary and Backup units. When local certificates are copied to the Backup unit, the associated private keys are also copied. Because the connection between the Primary and Backup units is typically protected, this is generally not a security concern.

Tip: *A compromise between the convenience of synchronizing certificates and the added security of not synchronizing certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.*

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then trigger a test failover by logging into the Primary unit and doing a restart. The Backup SonicWALL security appliance should quickly take over.

From your management workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet – note that the Backup SonicWALL, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Backup SonicWALL's unique LAN IP address. The management interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the management interface. If stateful synchronization is enabled (automatically disabling preempt mode), the management GUI should still display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure correct configuration.

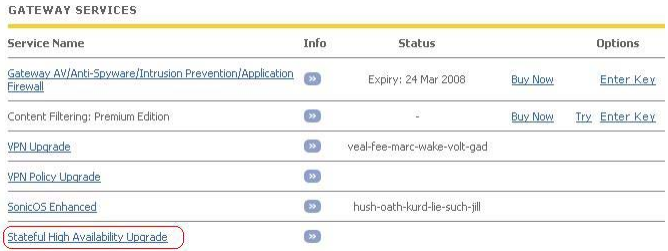
Synchronizing Firmware

Selecting the **Synchronize Firmware Upload and Reboot** checkbox allows the Primary and Backup SonicWALL security appliances in HA mode to have firmware uploaded on both devices at once, in staggered sequence to ensure that security is always maintained. During the firmware upload and reboot, you are notified via a message dialog box that the firmware is loaded on the Backup SonicWALL security appliance, and then the Primary SonicWALL security appliance. You initiate this process by clicking on the **Synchronize Firmware** button.

Configuring HA License Overview

You can configure HA license synchronization by associating two SonicWALL security appliances as HA Primary and HA Secondary on MySonicWALL. Note that the Backup appliance of your HA pair is referred to as the HA Secondary unit on MySonicWALL.

You must purchase a single set of security services licenses for the HA Primary appliance. To use Stateful HA, you must first activate the Stateful High Availability Upgrade license for the primary unit in SonicOS. This is automatic if your appliance is connected to the Internet. See *Registering and Licensing Your Appliance on MySonicWALL* - page 10.



License synchronization is used during HA so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable HA, you can use the SonicOS UI to configure your two appliances as a HA pair in Active/Idle mode.

MySonicWALL provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. You can associate two units that are both already registered. Or, you can select a registered unit and then add a new appliance with which to associate it.

Note that after registering new SonicWALL appliances on MySonicWALL, you must also register each appliance from the SonicOS management interface by clicking the registration link on the **System** > **Status** page. This allows each unit to synchronize with the SonicWALL license server and share licenses with the associated appliance.

Associating Pre-Registered Appliances

To associate two already-registered SonicWALL security appliances so that they can use HA license synchronization, perform the following steps:

1. Login to MySonicWALL.
2. In the left navigation bar, click **My Products**.
3. On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the parent, or primary, unit. Click the product **name** or **serial number**.
4. On the Service Management - Associated Products page, scroll down to the Associated Products section.
5. Under Associated Products, click **HA Secondary**.
6. On the My Product - Associated Products page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the appliance that you want to associate as the child/secondary/backup unit.
7. Select the group from the **Product Group** drop-down list. The product group setting specifies the MySonicWALL users who can upgrade or modify the appliance.
8. Click **Register**.

If You Are Following Scenario...	Proceed to Section:
B - NAT with State Sync Pair	*Additional Deployment Configuration* - page 35

Configuring L2 Bridge Mode

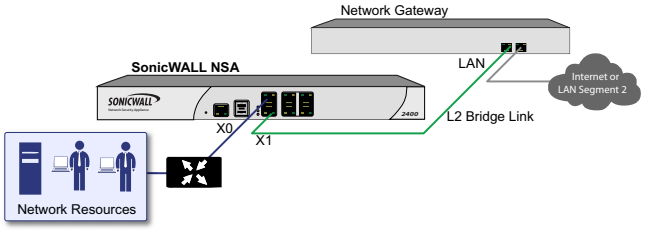
This section provides instructions to configure the SonicWALL NSA appliance in tandem with an existing Internet gateway device. This section is relevant to users following deployment **scenario C**.

This section contains the following subsections:

- *Connection Overview* - page 32
- *Configuring the Primary Bridge Interface* - page 32
- *Configuring the Secondary Bridge Interface* - page 32

Connection Overview

Connect the X1 port on your SonicWALL NSA 2400 to the LAN port on your existing Internet gateway device. Then connect the X0 port on your SonicWALL to your LAN.



Configuring the Primary Bridge Interface

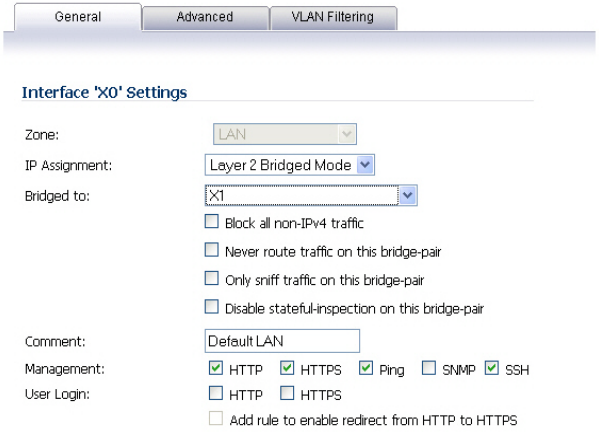
The primary bridge interface is your existing Internet gateway device. The only step involved in setting up your primary bridge interface is to ensure that the WAN interface is configured for a static IP address. You will need this static IP address when configuring the secondary bridge.

Note: *The primary bridge interface must have a static IP assignment.*

Configuring the Secondary Bridge Interface

Complete the following steps to configure the SonicWALL appliance:

1. Navigate to **Network** > **Interfaces**.
2. Click the Configure icon in the right column of the X0 (LAN) interface.



3. In the **IP Assignment** drop-down list, select **Layer 2 Bridged Mode**.
4. In the **Bridged to** drop-down list, select the **X1** interface.
5. Configure management options (HTTP, HTTPS, Ping, SNMP, SSH, User logins, or HTTP redirects).

Note: *Do not enable **Never route traffic on the bridge-pair** unless your network topology requires that all packets entering the L2 Bridge remain on the L2 Bridge segments.*

*You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.*

If You Are Following Scenario...	Proceed to Section:
C - L2 Bridge Mode	*Additional Deployment Configuration* - page 35

Additional Deployment Configuration

4

In this Section:

This section provides basic configuration information to begin building network security policies for your deployment. This section also contains several SonicOS diagnostic tools and a deployment configuration reference checklist.

- *Creating Network Access Rules* - page 36
- *Creating a NAT Policy* - page 38
  - *Creating Address Objects* - page 39
  - *Configuring NAT Policies* - page 40
- *Enabling Security Services in SonicOS* - page 41
- *Enforcing Security Services on Network Zones* - page 45
- *Deploying SonicPoints for Wireless Access* - page 46
- *Troubleshooting Diagnostic Tools* - page 51
- *Deployment Configuration Reference Checklist* - page 53

Creating Network Access Rules

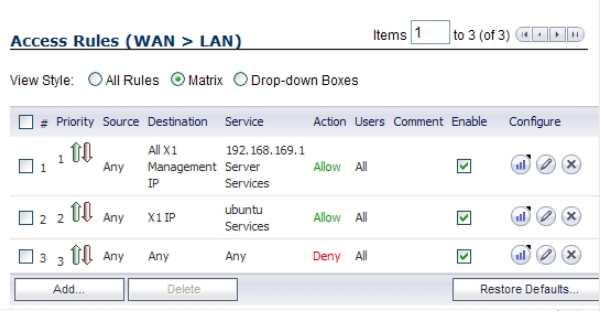
A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of access rules, a simpler and more intuitive process than following a strict physical interface scheme.

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the SonicWALL security appliance:

Originating Zone	Destination Zone	Action
LAN, WLAN	WAN, DMZ	Allow
DMZ	WAN	Allow
WAN	DMZ	Deny
WAN and DMZ	LAN or WLAN	Deny

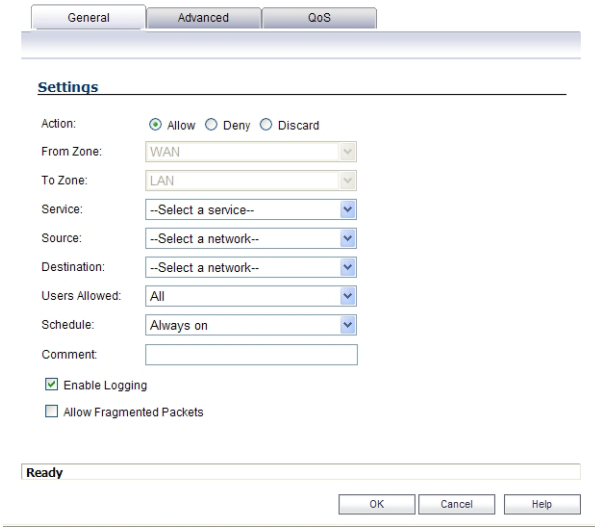
To create an access rule:

1. On the **Firewall** > **Access Rules** page in the matrix view, select two zones that will be bridged by this new rule.
2. On the Access Rules page, click **Add**.


Access Rules (WAN > LAN)
Items 1 to 3 (of 3)
View Style: All Rules Matrix Drop-down Boxes
Priority Source Destination Service Action Users Comment Enable Configure
1 1 Any All X1 Management IP 192.168.169.1 Server Services Allow All
2 2 Any X1 IP ubuntu Services Allow All
3 3 Any Any Any Deny All
Add... Delete Restore Defaults...

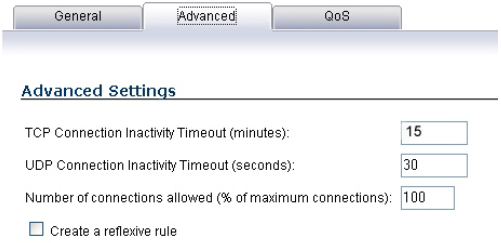
The access rules are sorted from the most specific at the top to the least specific at the bottom of the table. At the bottom of the table is the **Any** rule.

3. In the Add Rule page in the **General** tab, select **Allow** or **Deny** or **Discard** from the **Action** list to permit or block IP traffic.



- Select the service or group of services affected by the access rule from the **Service** drop-down list. If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
- Select the source of the traffic affected by the access rule from the **Source** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
- Select the destination of the traffic affected by the access rule from the **Destination** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
- Select a user or user group from the **Users Allowed** drop-down list.
- Select a schedule from the **Schedule** drop-down list. The default schedule is **Always on**.
- Enter any comments to help identify the access rule in the **Comments** field.

4. Click on the **Advanced** tab.



- In the **TCP Connection Inactivity Timeout (minutes)** field, set the length of TCP inactivity after which the access rule will time out. The default value is **15** minutes.
- In the **UDP Connection Inactivity Timeout (minutes)** field, set the length of UDP inactivity after which the access rule will time out. The default value is **30** minutes.
- In the **Number of connections allowed (% of maximum connections)** field, specify the percentage of maximum connections that is allowed by this access rule. The default is 100%.
- Select **Create a reflexive rule** to create a matching access rule for the opposite direction, that is, from your destination back to your source.

5. Click on the **QoS** tab to apply DSCP or 802.1p Quality of Service coloring/marking to traffic governed by this rule. See the *SonicOS Enhanced Administrator's Guide* for more information on managing QoS marking in access rules.
6. Click **OK** to add the rule.

Creating a NAT Policy

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to perform Many-to-One NAT between the systems on the LAN and the IP address of the WAN interface. The appliance does not perform NAT by default when traffic crosses between the other interfaces.

You can create multiple NAT policies on a SonicWALL running SonicOS Enhanced for the same object – for instance, you can specify that an internal server uses one IP address when accessing Telnet servers, and uses a different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to access multiple internal servers from the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

Before configuring NAT Policies, you must create all Address Objects that will be referenced by the policy. For instance, if you are creating a One-to-One NAT policy, first create Address Objects for your public and private IP addresses.

Address Objects are one of four object classes (Address, User, Service and Schedule) in SonicOS Enhanced. Once you define an Address Object, it becomes available for use wherever applicable throughout the SonicOS management interface. For example, consider an internal Web server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, you can create an Address Object to store the Web server's IP address. This Address Object, "My Web Server", can then be used in any configuration screen that employs Address Objects as a defining criterion.

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host –** Host Address Objects define a single host by its IP address.
- **Range –** Range Address Objects define a range of contiguous IP addresses.
- **Network –** Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask.
- **MAC Address –** MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address.
- **FQDN Address –** FQDN Address Objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as www.sonicwall.com.

SonicOS Enhanced provides a number of default Address Objects that cannot be modified or deleted. You can use the default Address Objects when creating a NAT policy, or you can create custom Address Objects to use. All Address Objects are available in the drop-down lists when creating a NAT policy.

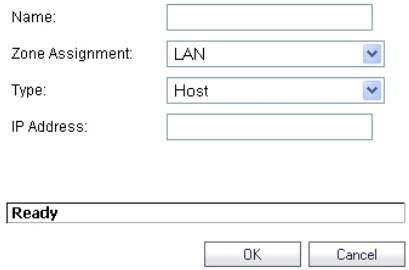
Creating Address Objects

The **Network** > **Address Objects** page allows you to create and manage your Address Objects. You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** – displays all configured Address Objects.
- **Custom Address Objects** – displays Address Objects with custom properties.
- **Default Address Objects** – displays Address Objects configured by default on the SonicWALL security appliance.

To add an Address Object:

1. Navigate to the **Network** > **Address Objects** page.
2. Below the **Address Objects** table, click **Add**.
3. In the **Add Address Object** dialog box, enter a name for the Address Object in the **Name** field.



4. Select the zone to assign to the Address Object from the **Zone Assignment** drop-down list.
5. Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.
   - For **Host**, enter the IP address in the **IP Address** field.
   - For **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
   - For **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.
   - For **MAC**, enter the MAC address and netmask in the **Network** and **MAC Address** field.
   - For **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.
6. Click **OK**.

Configuring NAT Policies

NAT policies allow you to control Network Address Translation based on matching combinations of Source IP address, Destination IP address and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously. The following NAT configurations are available in SonicOS Enhanced:

- Many-to-One NAT Policy
- Many-to-Many NAT Policy
- One-to-One NAT Policy for Outbound Traffic
- One-to-One NAT Policy for Inbound Traffic (Reflexive)
- One-to-Many NAT Load Balancing
- Inbound Port Address Translation via One-to-One NAT Policy
- Inbound Port Address Translation via WAN IP Address

This section describes how to configure a One-to-One NAT policy. One-to-One is the most common NAT policy used to route traffic to an internal server, such as a Web Server. Most of the time, this means that incoming requests from external IPs are translated from the IP address of the SonicWALL security appliance WAN port to the IP address of the internal web server.

For other NAT configurations, see the *SonicOS Enhanced Administrator's Guide*.

An example configuration illustrates the use of the fields in the Add NAT Policy procedure. To add a One-to-One NAT policy that allows all Internet traffic to be routed through a public IP address, two policies are needed: one for the outbound traffic, and one for the inbound traffic. To add both parts of a One-to-One NAT policy, perform the following steps:

1. Navigate to the **Network** > **NAT** Policies page. Click **Add**. The **Add NAT Policy** dialog box displays.
2. For **Original Source**, select **Any**.
3. For **Translated Source**, select **Original**.
4. For **Original Destination**, select **X0 IP**.
5. For **Translated Destination**, select **Create new address object** and create a new address object using **WAN** for Zone Assignment and **Host** for Type.
6. For **Original Service**, select **HTTP**.
7. For **Translated Service,** select **Original**.
8. For **Inbound Interface**, select **X0**.
9. For **Outbound Interface**, select **Any**.
10. For **Comment**, enter a short description.
11. Select the **Enable NAT Policy** checkbox.
12. Select the **Create a reflexive policy** checkbox if you want a matching NAT Policy to be automatically created in the opposite direction. This will create the outbound as well as the inbound policies.
13. Click **OK**.

Policies for subnets behind the other interfaces of the SonicWALL security appliance can be created by emulating these steps. Create a new NAT policy in which you adjust the source interface and specify the **Original Source**: the subnet behind that interface.

Enabling Security Services in SonicOS

SonicWALL security services are key components of threat management in SonicOS. The core security services are Gateway Anti-Virus, Intrusion Prevention Services, and Anti-Spyware.

You must enable each security service individually in the SonicOS user interface. See the following procedures to enable and configure the three security services that must be enabled:

- *Activating Licenses in SonicOS* - page 41
- *Configuring Security Services* - page 42
- *Enforcing Security Services on Network Zones* - page 45
- *Security Service Dashboard* - page 46

Activating Licenses in SonicOS

After completing the registration process in SonicOS, you must perform the following tasks to activate your licenses and enable your licensed services from within the SonicOS user interface:

- Activate licenses
- Enable security services
- Apply services to network zones

To activate licensed services in SonicOS, you can enter the license keyset manually, or you can synchronize all licenses at once with MySonicWALL.

The Setup Wizard automatically synchronizes all licenses with MySonicWALL if the appliance has Internet access during initial setup. If initial setup is already complete, you can synchronize licenses from the **System** > **Licenses** page.

Manual upgrade using the license keyset is useful when your appliance is not connected to the Internet. The license keyset includes all license keys for services or software enabled on MySonicWALL. It is available on <http://www.sonicwall.com> at the top of the Service Management page for your SonicWALL NSA appliance.

To activate licenses in SonicOS:

1. Navigate to the **System** > **Licenses** page.
2. Under Manage Security Services Online do one of the following:
   - Enter your MySonicWALL credentials, then click the **Synchronize** button to synchronize licenses with MySonicWALL.
   - Paste the license keyset into the **Manual Upgrade Keyset** field.
3. Click **Submit**.

Configuring Security Services

SonicWALL security services are key components of threat management in SonicOS. The core security services are Gateway Anti-Virus, Intrusion Prevention Services, and Anti-Spyware.

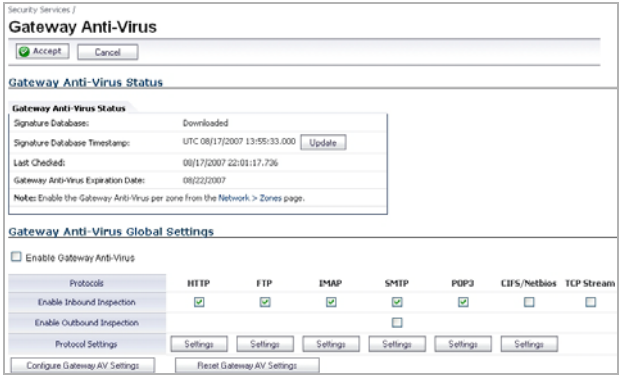
You must enable each security service individually in the SonicOS user interface.

- *Enabling Gateway Anti-Virus* - page 43
- *Enabling Intrusion Prevention Services* - page 43
- *Enabling Anti-Spyware* - page 44
- *Enabling Comprehensive Anti-Spam Service* - page 44
- *Enabling Content Filtering Service* - page 45

Enabling Gateway Anti-Virus

To enable Gateway Anti-Virus in SonicOS:

1. Navigate to **Security Services** > **Gateway Anti-Virus**.
2. Select the **Enable Gateway Anti-Virus** checkbox.
3. Choose to **Enable Inbound Inspection** and **Enable Outbound Inspection** on the desired protocols.

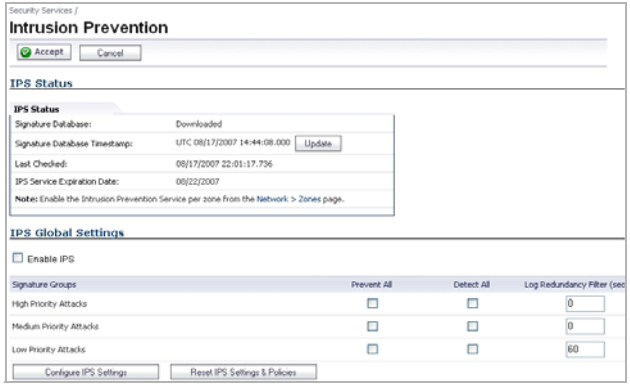


4. Click the **Accept** button.

Enabling Intrusion Prevention Services

To enable Intrusion Prevention Services in SonicOS:

1. Navigate to **Security Services** > **Intrusion Prevention**.
2. Select the **Enable Intrusion Prevention** checkbox.
3. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes for each attack priority that you want to prevent. Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and **Medium Priority Attacks** protects your network against the most dangerous and disruptive attacks.

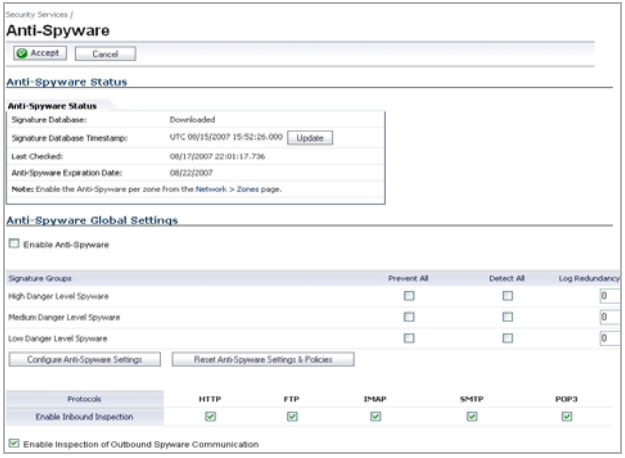


4. Click the **Accept** button.

Enabling Anti-Spyware

To enable Anti-Spyware in SonicOS:

1. Navigate to the **Security Services** > **Anti-Spyware** page.
2. Select the **Enable Anti-Spyware** checkbox.
3. Select the **Prevent All** and **Detect All** checkboxes for each spyware danger level that you want to prevent.
4. Select the inbound **Protocols** you wish to inspect.
5. Select the **Enable Inspection of Outbound Spyware Communication** checkbox to enforce signature inspection on outbound traffic.



6. Click the **Accept** button.

Enabling Comprehensive Anti-Spam Service

To enable Anti-Spam in SonicOS:

1. Navigate to the **Anti-Spam > Settings** page.

Note: *If the service is not registered yet, click the SonicWALL Comprehensive Anti-Spam Service Trial link or register the service on MySonicWALL.*

2. Select the **Enable Anti-Spam Service** checkbox.

3. Email System Detection will attempt to configure your service automatically. Alternatively, you may scroll down to configure **Advanced Options**, including service probes and your mail server address and port.
4. Click the **Accept** button to complete the setup process.

Enabling Content Filtering Service

Content Filtering Service (CFS) Bypass for Administrators

The **Do not bypass CFS blocking for the administrator** checkbox controls content filtering for administrators. By default, when the administrator (“admin” user) is logged into the SonicOS management interface from a system, CFS blocking is suspended for that system’s IP address for the duration of the authenticated session. If you prefer to provide content filtering and apply CFS policies to the IP address of the administrator’s system, perform the following steps:

1. Select the **Do not bypass CFS blocking for the Administrator checkbox**.
2. Click **Accept**.

Enabling and Adding to the CFS Exclusion List

To enable the CFS Exclusion List and add a range of IP addresses to it, perform the following steps:

1. Select the **Enable CFS Exclusion List** checkbox.
2. Click **Add**. The **Add CFS Range Entry** window is displayed.
3. Enter the first IP address in the excluded range into the **IP Address From:** field and the last address into the **IP Address To:** field.
4. Click **OK**. The IP address range is added to the CFS Exclusion List.
5. On the **Security Services > Content Filter** page, click **Accept**.

Enforcing Security Services on Network Zones

A network zone is a logical group of one or more interfaces to which you can apply security rules to regulate traffic passing from one zone to another zone.

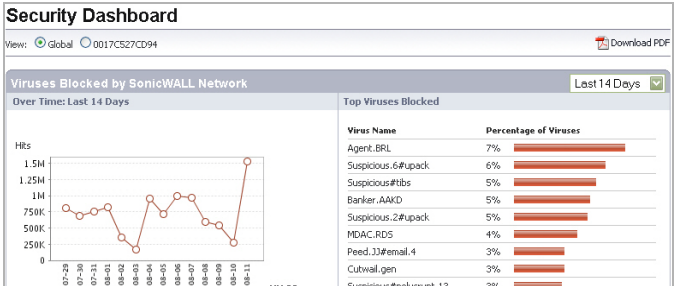
Security services such as Gateway Anti-Virus are automatically applied to the LAN and WAN network zones. To protect other zones such as the DMZ or Wireless LAN (WLAN), you must apply the security services to the network zones. For example, you can configure SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic.

To apply services to network zones:

1. Navigate to the **Network** > **Zones** page.
2. In the Zone Settings table, click the **Configure** icon for the zone where you want to apply security services.
3. In the Edit Zone dialog box on the General tab, select the checkboxes for the security services to enable on this zone.
4. Click **OK**.
5. To enable security services on other zones, repeat steps 2 through step 4 for each zone.

Security Service Dashboard

The SonicOS Security Dashboard displays local and global statistics on blocked threats. The Security Dashboard is accessable from the **System > Security Dashboard** page in the SonicOS management interface.



Deploying SonicPoints for Wireless Access

This section describes how to configure SonicPoints with the SonicWALL NSA 2400. See the following subsections:

- *Updating SonicPoint Firmware* - page 46
- *Configuring SonicPoint Provisioning Profiles* - page 47
- *Configuring a Wireless Zone* - page 48
- *Assigning an Interface to the Wireless Zone* - page 50
- *Connecting the SonicPoint* - page 50

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances to provide wireless access throughout your enterprise. The SonicPoint section of the SonicOS management interface lets you manage the SonicPoints connected to your system.

Before you can manage SonicPoints in the Management Interface, you must first:

- Verify that the SonicPoint image is downloaded to your SonicWALL security appliance.
- Configure your SonicPoint provisioning profiles.
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign an interface to the Wireless zone.
- Attach the SonicPoints to the interface in the Wireless zone and test.

Updating SonicPoint Firmware

If your SonicWALL appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint image from the SonicWALL server when you connect a SonicPoint device. Otherwise, see the *SonicOS Enhanced Administrator's Guide* for the correct procedure.

Configuring SonicPoint Provisioning Profiles

SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. When a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone. SonicOS includes a default SonicPoint profile, named SonicPoint. You can modify this profile or create a new one.

To add a new profile, click **Add** below the list of SonicPoint provisioning profiles. To edit an existing profile, select the profile and click the **Configure** icon in the same line as the profile you are editing.

1. In the Add/Edit SonicPoint Profile window on the **General** tab:
   - Select **Enable SonicPoint**.
   - Enter a **Name Prefix** to be used as the first part of the name for each SonicPoint provisioned.
   - Select the **Country Code** for where the SonicPoints are operating.
2. In the **802.11g Radio** tab:
   - Select **Enable Radio**.
   - Select a schedule for the radio to be enabled from the drop-down list.
   - For **Radio Mode**, select the speed that the SonicPoint will operate on. You can choose from the following:
     - 11Mbps - 802.11b
     - 54 Mbps - 802.11g
     - 108 Mbps - Turbo G

     If you choose Turbo mode, all users in your company must use wireless access cards that support Turbo mode.
   - For **Channel**, use AutoChannel unless you have a reason to use or avoid specific channels.
   - Enter a recognizable string for the **SSID** of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.
   - Under **ACL Enforcement**, select **Enable MAC Filter List** to enforce Access Control by allowing or denying traffic from specific devices. Select a MAC address object group from the **Allow List** to automatically allow traffic from all devices with MAC addresses in the group. Select a MAC address group from the **Deny List** to automatically deny traffic from all devices with MAC addresses in the group. The Deny List is enforced before the Allow List.

- Under **WEP/WPA Encryption**, select the **Authentication Type** for your wireless network. SonicWALL recommends using **WPA2** as the authentication type.

Note: *WPA2 is a more secure replacement for the older WEP and WPA standards.*

- Fill in the fields specific to the authentication type that you selected. The remaining fields change depending on the selected authentication type.

3. In the **802.11g Adv** tab, configure the advanced radio settings for the 802.11g radio. For most 802.11g advanced options, the default settings give optimum performance. For a full description of the fields on this tab, see the *SonicOS Enhanced Administrator's Guide*.
4. In the **802.11a Radio** and **802.11a Adv** tabs, configure the settings for the operation of the 802.11a radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.
   The settings in the **802.11a Radio** and **802.11a Advanced** tabs are similar to the settings in the **802.11g Radio** and **802.11g Advanced** tabs.
5. When finished, click **OK**.

Configuring a Wireless Zone

You can configure a wireless zone on the **Network** > **Zones** page. Typically, you will configure the WLAN zone for use with SonicPoints.

1. On the **Network** > **Zones** page in the **WLAN** row, click the icon in the **Configure** column.
2. In the Edit Zone dialog box on the **General** tab, the **Allow Interface Trust** setting automates the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the WLAN Zone has both the **X2** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the WLAN Zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.
3. Select the checkboxes for the security services to enable on this zone. Typically you would enable **Gateway Anti-Virus**, **IPS**, and **Anti-Spyware**. If your wireless clients are all running SonicWALL Client Anti-Virus, select **Enable Client AV Enforcement Service**.

4. Click the **Wireless** tab.
   - In the **Wireless Settings** section, select **Only allow traffic generated by a SonicPoint** to allow only traffic from SonicWALL SonicPoints to enter the WLAN Zone interface. This provides maximum security on your WLAN. Uncheck this option if you want to allow any traffic on your WLAN Zone regardless of whether or not it is from a SonicPoint.
   - Select **SSL VPN Enforcement** to require that all traffic that enters into the WLAN Zone be authenticated through a SonicWALL SSL VPN appliance.

Note: *SSL VPN Enforcement allows the added security of one-time passwords when using a SonicWALL SSL VPN appliance.*

   - In the **SSL VPN Server** list, select an address object to direct traffic to the SonicWALL SSL VPN appliance.
   - In the **SSL VPN Service** list, select the service or group of services that you want to allow for clients authenticated through the SSL VPN.
   - If your wireless network is already running WiFiSec, you can select **WiFiSec Enforcement** to require that all traffic that enters into the WLAN Zone interface be either IPsec traffic, WPA traffic, or both.

Note: *If you have configured WPA2 as your authentication type, you do not need to enable WiFiSec.*

   If you have enabled **WiFiSec Enforcement**, you can specify the following:
   - Select **WiFiSec Exception Service** to select services that are allowed to bypass the WiFiSec enforcement.
   - Select **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** to require WiFiSec security for all wireless connections through the WLAN zone that are part of a Site-to-Site VPN.
   - If you wish to run WPA or WPA2 in addition to WiFiSec, you can select **Trust WPA/WPA2 traffic as WiFiSec** to accept WPA and WPA2 as allowable alternatives to WiFiSec.
   - Under **SonicPoint Settings**, select the **SonicPoint Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.
5. Optionally configure the settings on the **Guest Services** tab. For information about configuring Guest Services, see the *SonicOS Enhanced Administrator's Guide*.
6. When finished, click **OK**.

Assigning an Interface to the Wireless Zone

Once the wireless zone is configured, you can assign an interface to it. This is the interface where you will connect the SonicPoint.

1. On the **Network** > **Interfaces** page, click the **Configure** icon in the row for the interface that you want to use, for example, X3. The interface must be unassigned.
2. In the Edit Interface dialog box on the **General** tab, select **WLAN** or the zone that you created from the **Zone** drop-down list. Additional fields are displayed.
3. Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.
4. In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface.
5. If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
6. If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
7. Click **OK**.

Connecting the SonicPoint

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP Address 192.168.1.20, username: **admin**, password: **password**). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint locates a peer SonicOS device via the SonicWALL Discovery Protocol, the two units perform an encrypted exchange and the profile assigned to the relevant wireless zone is used to automatically configure (provision) the newly added SonicPoint unit.

As part of the provisioning process, SonicOS assigns the discovered SonicPoint device a unique name, records the SonicPoint's MAC address and the interface and zone on which it was discovered, and uses the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support.

To connect the SonicPoint:

1. Using a Cat-5 Ethernet cable, connect the SonicPoint to the interface that you configured. Then connect the SonicPoint to a power source.
2. In the SonicOS user interface on the **SonicPoint** > **SonicPoints** page, click the **Synchronize SonicPoints** button. The SonicWALL appliance downloads a SonicPoint image from the SonicWALL back-end server.
3. Follow the instructions in the SonicPoint wizard. Be sure to select the same authentication type and enter the same keys or password that you configured in SonicOS.

For more information about wireless configuration, see the *SonicOS Enhanced Administrator's Guide*.

Troubleshooting Diagnostic Tools

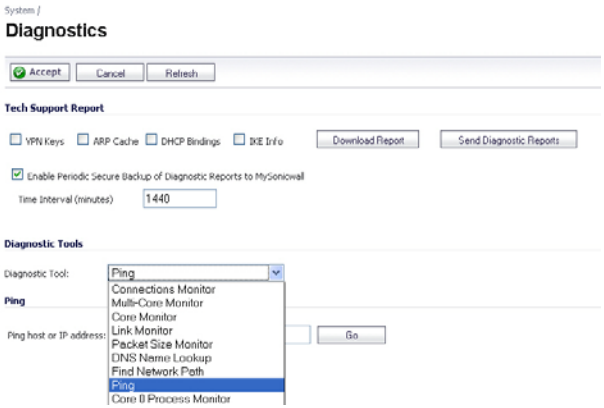
SonicOS provides a number of diagnostic tools to help you maintain your network and troubleshoot problems. Several tools can be accessed on the **System** > **Diagnostics** page, and others are available on other screens.

This section contains the following subsections:

- *Using Ping* - page 51
- *Using the Active Connections Monitor* - page 52
- *Using Log > View* - page 52

Using Ping

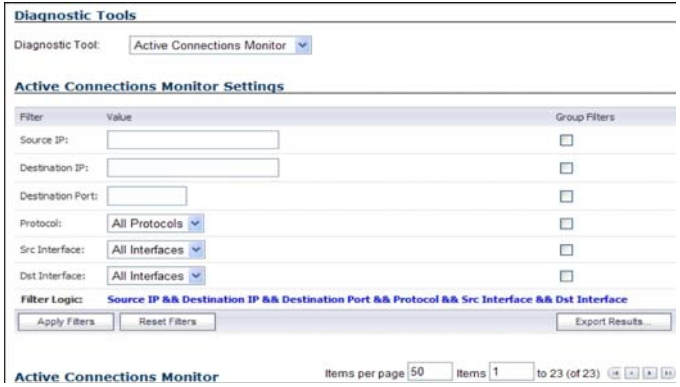
Ping is available on the **System** > **Diagnostics** page.



The Ping test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

Using the Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the SonicWALL security appliance. This tool is available on the **Systems** > **Diagnostics** page.



You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface** and **Dst Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

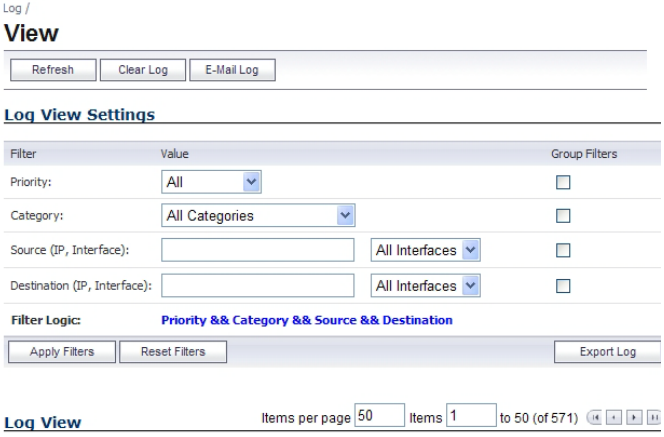
The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.

Using Log > View

The SonicWALL security appliance maintains an Event log for tracking potential security threats. You can view the log in the **Log** > **View** page, or it can be automatically sent to an email address for convenience and archiving. The log is displayed in a table and can be sorted by column.

You can filter the results to display only event logs matching certain criteria. You can filter by **Priority**, **Category**, **Source** (**IP** or **Interface**), and **Destination** (**IP** or **Interface**).

The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.



Deployment Configuration Reference Checklist

Use this checklist to find more information about various deployment tasks within the *SonicOS Enhanced Administrator's Guide*.

For this Task...	See this Chapter...
Inspecting the rule base for inbound and outbound rules	Configuring Access Rules
Setting logging levels	Configuring Log Categories (“Logging Level” section)
Configuring threat prevention on all used zones	Configuring Zones (“Enabling SonicWALL Security Services on Zones“ section)
Configuring Web filtering protection	Configuring SonicWALL Content Filtering Service
Changing administrator login	Configuring Administration Settings ("Administrator Name & Password“ section)
Setting administrator email	Configuring Log Automation (“Email Log Automation“ section)
Disabling HTTP and ping access	Configuring Interfaces (“Configuring Advanced Settings for the Interfaces“ section)
Disabling or enabling DHCP	Setting Up the DHCP Server
Configuring user management	Managing Users and Authentication Settings
Configuring VPN policies	Configuring VPN Policies
Securing wireless access	Managing SonicPoints

Support and Training Options

5

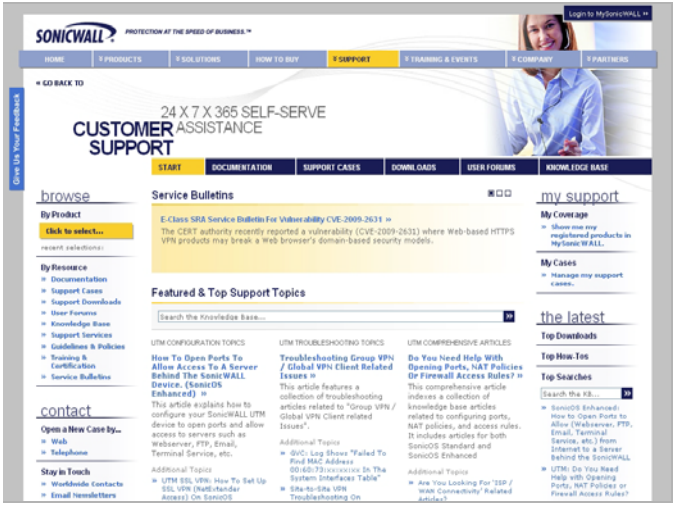
In this Section:

This section provides overviews of customer support and training options for the SonicWALL NSA 2400.

- *Customer Support* - page 56
- *Knowledge Base* - page 56
- *SonicWALL Live Product Demos* - page 57
- *User Forums* - page 58
- *Training* - page 59
- *Related Documentation* - page 60
- *SonicWALL Secure Wireless Network Integrated Solutions Guide* - page 61

Customer Support

For answers to all your support questions visit the SonicWALL support Web site at <http://www.sonicwall.com/us/Support.html> where you will find featured support topics, tutorials, and more. If you need further assistance, SonicWALL offers telephone, email, and Web-based support to customers with valid Warranty Support or a purchased support contract. Please review our Warranty Support Policy for product coverage.

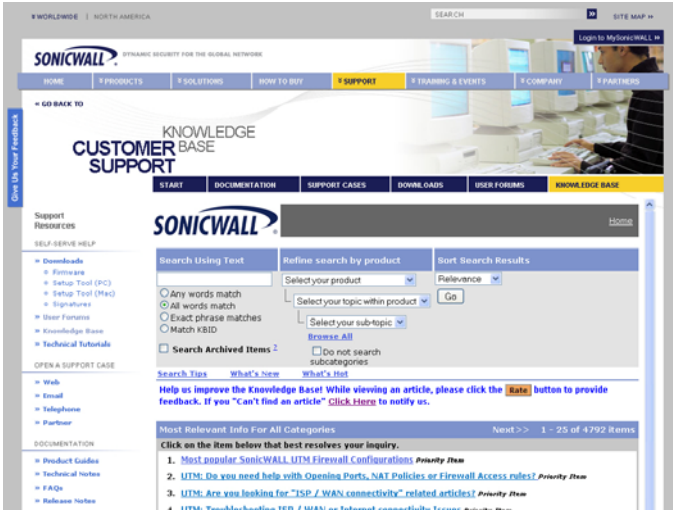


Knowledge Base

The Knowledge Base allows users to search for SonicWALL documents based on the following types of search tools:

- Browse
- Search for keywords
- Full-text search

For further information, navigate to the **Support** > **Knowledge Base** page at: <http://www.mysonicwall.com/>

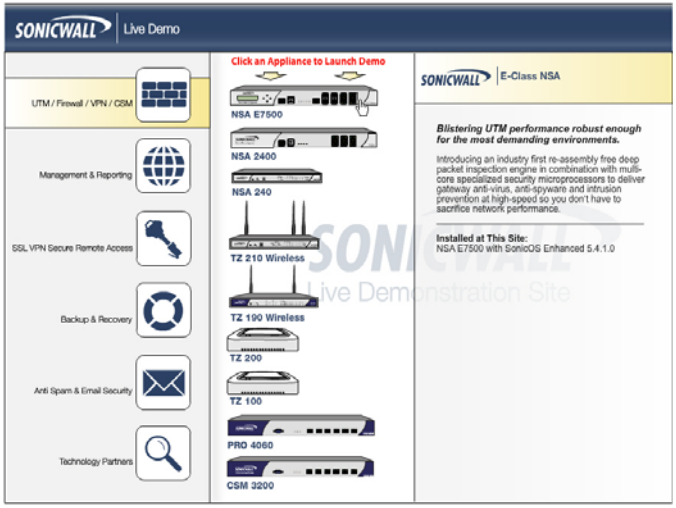


SonicWALL Live Product Demos

Get the most out of your appliance with the complete line of SonicWALL products. The SonicWALL Live Demo Site provides free test drives of SonicWALL security products and services through interactive live product installations:

- Unified Threat Management Platform
- Secure Cellular Wireless
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Secure Wireless Solutions
- Email Security
- SonicWALL GMS and ViewPoint

For further information, visit:
<http://livedemo.sonicwall.com/>


SONICWALL
Live Demo
UTM / Firewall / VPN / CSM
Management & Reporting
SSL VPN Secure Remote Access
Backup & Recovery
Anti Spam & Email Security
Technology Partners
Click an Appliance to Launch Demo
NSA E7500
NSA 2400
NSA 240
TZ 210 Wireless
TZ 190 Wireless
TZ 200
TZ 100
PRO 4060
CSM 3200
SONICWALL
E-Class NSA
Blistering UTM performance robust enough for the most demanding environments.
Introducing an industry first re-assembly free deep packet inspection engine in combination with multi-core specialized security microprocessors to deliver gateway anti-virus, anti-spyware and intrusion prevention at high-speed so you don't have to sacrifice network performance.
Installed at This Site:
NSA E7500 with SonicOS Enhanced 5.4.1.0
Live Demonstration Site

User Forums

The SonicWALL User Forums is a resource that provides users the ability to communicate and discuss a variety of security and appliance subject matters. In this forum, the following categories are available for users:

- Content Security Manager topics
- Continuous Data Protection topics
- Email Security topics
- Firewall topics
- Network Anti-Virus topics
- Security Services and Content Filtering topics
- SonicWALL GMS and Viewpoint topics
- SonicPoint and Wireless topics
- SSL VPN topics
- Wireless WAN - 3G Capability topics
- VPN Client topics
- VPN site-to-site and interoperability topics

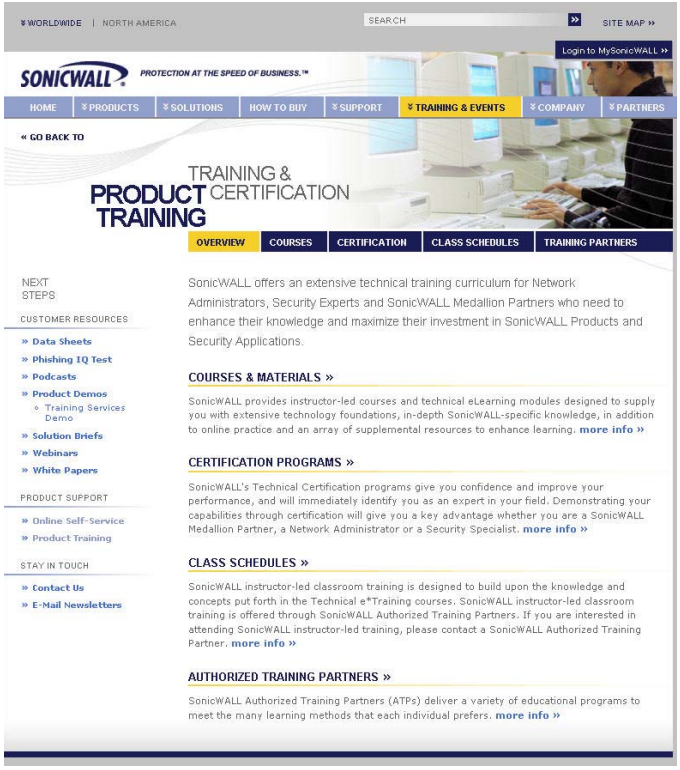
For further information, visit:
<https://forum.sonicwall.com/>

Training

SonicWALL offers an extensive sales and technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications. SonicWALL Training provides the following resources for its customers:

- E-Training
- Instructor-Led Training
- Custom Training
- Technical Certification
- Authorized Training Partners

For further information, visit:
<http://www.sonicwall.com/us/support/training.html>

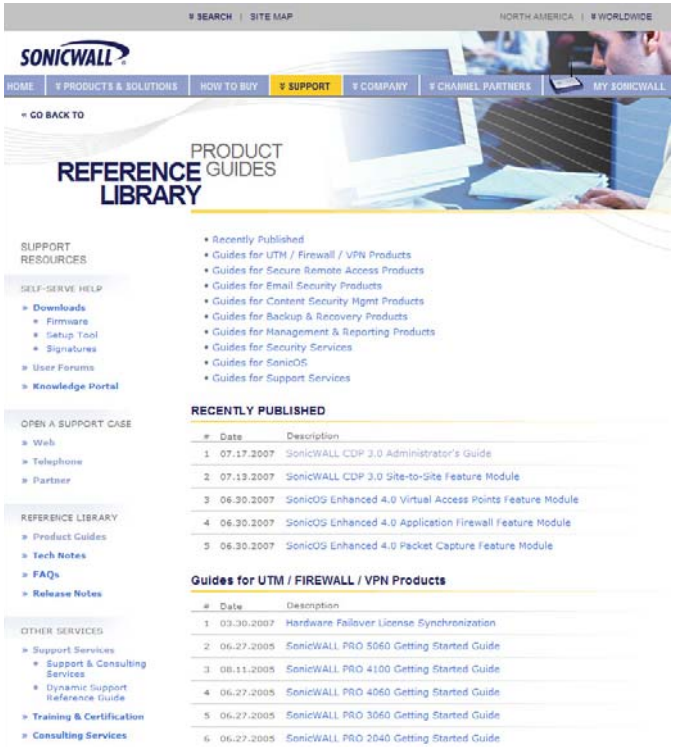

WORLDWIDE | NORTH AMERICA
SEARCH
SITE MAP »
Login to MySonicWALL »
SONICWALL
PROTECTION AT THE SPEED OF BUSINESS.™
HOME
PRODUCTS
SOLUTIONS
HOW TO BUY
SUPPORT
TRAINING & EVENTS
COMPANY
PARTNERS
« GO BACK TO
TRAINING &
PRODUCT CERTIFICATION
TRAINING
OVERVIEW
COURSES
CERTIFICATION
CLASS SCHEDULES
TRAINING PARTNERS
NEXT STEPS
CUSTOMER RESOURCES
» Data Sheets
» Phishing IQ Test
» Podcasts
» Product Demos
» Training Services Demo
» Solution Briefs
» Webinars
» White Papers
PRODUCT SUPPORT
» Online Self-Service
» Product Training
STAY IN TOUCH
» Contact Us
» E-Mail Newsletters
SonicWALL offers an extensive technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications.
COURSES & MATERIALS »
SonicWALL provides instructor-led courses and technical eLearning modules designed to supply you with extensive technology foundations, in-depth SonicWALL-specific knowledge, in addition to online practice and an array of supplemental resources to enhance learning. more info »
CERTIFICATION PROGRAMS »
SonicWALL's Technical Certification programs give you confidence and improve your performance, and will immediately identify you as an expert in your field. Demonstrating your capabilities through certification will give you a key advantage whether you are a SonicWALL Medallion Partner, a Network Administrator or a Security Specialist. more info »
CLASS SCHEDULES »
SonicWALL instructor-led classroom training is designed to build upon the knowledge and concepts put forth in the Technical e*Training courses. SonicWALL instructor-led classroom training is offered through SonicWALL Authorized Training Partners. If you are interested in attending SonicWALL instructor-led training, please contact a SonicWALL Authorized Training Partner. more info »
AUTHORIZED TRAINING PARTNERS »
SonicWALL Authorized Training Partners (ATPs) deliver a variety of educational programs to meet the many learning methods that each individual prefers. more info »

Related Documentation

See the following related documents for more information:

- *SonicOS Enhanced Administrator's Guide*
- *SonicOS Enhanced Release Notes*
- *SonicOS Enhanced Feature Modules*
  - Application Firewall
  - Dashboard
  - HA License Sync
  - Multiple Admin
  - NAT Load Balancing
  - Packet Capture
  - Radio Frequency Monitoring
  - Single Sign-On
  - SSL Control
  - Virtual Access Points
- *SonicWALL GMS Administrator's Guide*
- *SonicWALL GVC Administrator's Guide*
- *SonicWALL ViewPoint Administrator's Guide*
- *SonicWALL GAV Administrator's Guide*
- *SonicWALL IPS Administrator's Guide*
- *SonicWALL Anti-Spyware Administrator's Guide*
- *SonicWALL CFS Administrator's Guide*

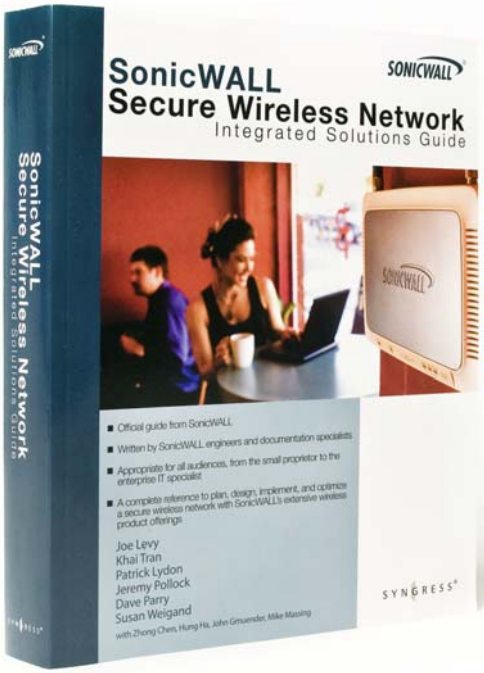
For further information, visit:
<http://www.sonicwall.com/us/support/289.html>



SonicWALL Secure Wireless Network Integrated Solutions Guide

Looking to go wireless? Have questions about what it takes to build a truly “secure” wireless network? Check out the SonicWALL Secure Wireless Network Integrated Solutions Guide. This book is the official guide to SonicWALL’s market-leading wireless networking and security devices.

This title is available in hardcopy at fine book retailers everywhere, or by ordering directly from Elsevier Publishing at: <http://www.elsevier.com>


SonicWALL
Secure Wireless Network
Integrated Solutions Guide
SONICWALL
SonicWALL
Secure Wireless Network
Integrated Solutions Guide
Official guide from SonicWALL
Written by SonicWALL engineers and documentation specialists
Appropriate for all audiences, from the small proprietor to the enterprise IT specialist
A complete reference to plan, design, implement, and optimize a secure wireless network with SonicWALL's extensive wireless product offerings
Joe Levy
Khai Tran
Patrick Lydon
Jeremy Pollock
Dave Parry
Susan Weigand
with Zhong Chen, Hung Ha, John Gmuender, Mike Massing
SYNGRESS

Product Safety and Regulatory Information

6

In this Section:

This section provides regulatory, trademark, and copyright information.

- *Safety and Regulatory Information* - page 64
- *Copyright Notice* - page 67
- *Trademarks* - page 67

Safety and Regulatory Information

Regulatory Model/Type	Product Name
1RK14-053 1RK25-084 1RK25-086	NSA 2400

Rack Mounting the SonicWALL

The above SonicWALL appliance is designed to be mounted in a standard 19-inch rack mount cabinet. The following conditions are required for proper installation:

- Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the application.
- Four mounting screws, compatible with the rack design, must be used and hand tightened to ensure secure installation. Choose a mounting location where all four mounting holes line up with those of the mounting bars of the 19-inch rack mount cabinet.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters and broadband amplifiers.
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
- Mount the SonicWALL appliances evenly in the rack in order to prevent a hazardous condition caused by uneven mechanical loading.
- Consideration must be given to the connection of the equipment to the supply circuit. The effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.
- Reliable grounding of rack-mounted equipment must be maintained. Particular attention must be given to power supply connections other than direct connections to the branch circuits such as power strips.
- If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum recommended ambient temperature shown above.

Lithium Battery Warning

The Lithium Battery used in the SonicWALL Internet security appliance may not be replaced by the user. The SonicWALL must be returned to a SonicWALL authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWALL Internet security appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the SonicWALL is located.

Safety and Regulatory Information in German

Weitere Hinweise zur Montage

Das SonicWALL Modell ist für eine Montage in einem standardmäßigen 19-Zoll-Rack konzipiert. Für eine ordnungsgemäße Montage sollten die folgenden Hinweise beachtet werden:

- Vergewissern Sie sich, dass das Rack für dieses Gerät geeignet ist und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- Verwenden Sie für eine sichere Montage vier passende Befestigungsschrauben, und ziehen Sie diese mit der Hand an. Wählen Sie einen Ort im 19-Zoll-Rack, wo alle vier Befestigungen der Montageschien verwendet werden.
- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Achten Sie darauf, das sich die Netzwerkkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden.
- Das beigefügte Netzkabel ist nur für den Gebrauch in Nordamerikas Vorgesehen. Für Kunden in der Europaïschen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Bringen Sie die SonicWALL waagerecht im Rack an, um mögliche Gefahren durch ungleiche mechanische Belastung zu vermeiden.
- Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts.
- Eine sichere Erdung der Geräte im Rack muss gewährleistet sein. Insbesondere muss auf nicht direkte Anschlüsse an Stromquellen geachtet werden wie z. B. bei Verwendung von Mehrfachsteckdosen.
- Wenn das Gerät in einem geschlossenen 19"-Gehäuse oder mit mehreren anderen Geräten eingesetzt ist, wird die Temperatur in der Gehäuse höher sein als die Umgebungstemperatur. Achten Sie darauf, daß die Umgebungstemperatur nicht mehr als 40° C beträgt.

Hinweis zur Lithiumbatterie

Die in der Internet Security Appliance von SonicWALL verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die SonicWALL in ein von SonicWALL autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der SonicWALL Internet Security Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der SonicWALL keine Kabel an, die aus dem Gebäude in dem sich das Gerät befindet ,herausgeführt werden.

FCC Part 15 Class A Notice

NOTE: This equipment was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. And if not installed and used in accordance with the instruction manual, the device may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

Caution: *Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user's authority to operate this equipment.*

BMSI Statement

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－ A

Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à toutes la norme NMB-003 du Canada.

Complies with EN 55022 Class A and CISPR22 Class A

Warning: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Declaration of Conformity
Application of council Directive 2004/108/EC (EMC) and 2006/95/EC (LVD)
Standards to which conformity is declared
EN 55022 (2006) +A1 (2007) Class A
EN 55024 (1998) +A1 (2001), +A2 (2003)
EN 61000-3-2 (2006)
EN 61000-3-3 (2008)

EN 60950-1 (2006) +A11
National Deviations: AR, AT, AU, BE, BR, CA, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IL, IN, IT, JP, KE, KR, MY, NL, NO, PL, SE, SG, SI, SK, US

Regulatory Information for Korea

	Ministry of Information and Telecommunication Certification Number Certification Number SWL-1RK14-053 SWL-1RK25-084 SWL-1RK25-086

All products with country code "" (blank) and "A" are made in the USA.
All products with country code "B" are made in China.
All products with country code "C" or "D" are made in Taiwan R.O.C.
All certificates held by Secuwide, Corp.

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Copyright Notice

© 2011 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions are subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Firefox is a trademark of the Mozilla Foundation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Notes

SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

P/N 232-001276-52
Rev A 01/11

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

©2011 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.